REMARKS

Claims 1-35 are currently pending in the subject application and are presently under consideration. Claims 1, 17, 26, 31 and 35 have been amended as shown at pages 2-7 of the Reply. In addition, claim 30 has been cancelled.

Applicants' representative thanks Examiner Jung for the courtesies extended during the telephonic interviews conducted on November 14, 2007. Examiner was contacted to discuss the rejections under 35 U.S.C. §101 and 35 U.S.C. §103(a). During the interview a set of amendments were agreed upon that addressed all of the rejections under 35 identified in the Office Action. Examiner indicated that further arguments relating to functional aspects of the claims in support of the amendments to overcome the 35 U.S.C. §101 were required. Examiner indicated that further search and consideration was required to determine if the claims would be allowed over the cited prior art.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-35 Under 35 U.S.C. §101

Claims 1-35 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Independent claims 1, 17, 26, 31 and 35 have been amended to recite embodiment on a computer readable storage medium, which clearly falls within the classes of statutory subject matter. Furthermore, independent claims 1, 17, 26, and 31, have been amended to recite that the message (encrypted or decrypted) is at least one of stored on a computer readable storage medium, displayed on a display device, employed by one or more processes executed on one or more processors, or transmitted between two or more processes executing on one or more processors. Employing keys to encrypt and decrypt messages requires a functional interrelationship among the keys and messages and the computer processes performed when utilizing the data. This clearly makes the resulting encrypted or decrypted message concrete, useful, and tangible, as it can be employed by a device or user. Moreover, independent claim 35 discloses that the data packet is stored on a computer readable storage medium clearly making it a concrete, useful, and tangible result that can be employed by a device or user.

II. Rejection of Claims 1-35 Under 35 U.S.C. §103(a)

Claims 1-35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Helland (http://www.microsoft.com/presspass/exec/flessner/04-11flessnerteched.mspx) and Bresson and IETF (http://tools.ietf.org/html/draft-ietf-sip-rfc2543bis-09). This rejection should be withdrawn for at least the following reason. Helland, Bresson, and IETF do not teach or suggest all the limitations of the subject claims.

> If a reference is cited that requires some modification in order to meet the claimed invention or requires some modification in order to be properly combined with another reference and such modification destroys the purpose or function of the invention disclosed in the reference, one of ordinary skill in the art would not have found a reason to make the claimed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The subject claims relate to secure exchange of information by employing encrypted keys. Existing multi-level encryption schemes rely on a third party acting as gateway to provide authentication and decryption keys. This allows for a compromised or malicious third party to have the ability to decrypt secured communications. The subject claims disclose a multi-level encrypted key scheme, not requiring a third party, whereby an asymmetrically encrypted initiator key is employed to encrypt authentication information, an asymmetrically encrypted key exchange key is employed to encrypt a dialog session key, and the dialog key is employed to encrypt a message body. In this manner the more complex asymmetrically encrypted keys can be employed to encrypt security information in order to simulate what would normally have been provided by a third party, thereby, providing a level of indirection. The more simply symmetrically encoded dialog key can be employed to encrypt the message body, requiring less processing overhead. When caching is employed to store decrypted keys at either or both ends of the information exchange, additional processing overhead can be saved. In this manner, avoiding a third party for key exchange that could possibly get compromised, while reducing processing requirements is achieved.

Independent claim 1 (and similarly independent claim 26) recites, *a service pair encryption component that employs an initiator private key to encrypt authentication information; a key exchange key encryption component that employs a target public key to encrypt a key exchange key; a dialog session key encryption component that employs the key*

exchange key to encrypt a dialog session key; a message body encryption component that employs the dialog session key to encrypt a message body; and, a message generator that generates an encrypted message based, at least in part, upon the encrypted authentication information, the encrypted key exchange key, the encrypted dialog session key and the encrypted message body. The subject claim clearly discloses an asymmetrically encrypted initiator key is employed to encrypt authentication information, an asymmetrically encrypted key exchange key is employed to encrypt a dialog session key, and the dialog key is employed to encrypt a message body. Helland, Bresson, and IETF do not teach or suggest such claimed features. Helland is a general discussion of technology trends and fails to discuss secured information exchange and encryption employing keys. Bresson discloses secured communication and techniques to prove authentication schemes. However, the cited reference only discloses an encrypted session key. It fails to disclose a multi-level key encryption scheme that employs asymmetric keys at a higher level and symmetric keys at a lower level to secure information exchange. Furthermore, it does not disclose employing a asymmetrically encrypted key to encrypt a symmetrically encrypted key as disclosed in the subject claim. IETF similar to Bresson discloses a single level encryption key. As such, Helland, Bresson, and IETF do not teach the novel features disclosed in the subject claim.

Independent claim 17, recites *a message receiver that receives an encrypted message; a service pair encryption component that employs an initiator public key to decrypt authentication information of the encrypted message; a key exchange key decryption component that employs a target private key to decrypt a key exchange key of the encrypted message, if the key exchange key is not stored in a cache; a dialog session key decryption component that employs the key exchange key to decrypt a dialog session key of the encrypted message, if the dialog session key is not stored in the cache; and, a message body decryption component that employs the decrypted or stored dialog session key to decrypt a message body of the encrypted message*. The subject claim discloses the receiving side of the information exchange, where a multi-level key encryption scheme is employed. As discussed above, the Helland, Bresson, and IETF fail to teach or suggest a multi-level key encryption scheme. Furthermore, the subject claim discloses that decrypted keys can be stored and employed when an encrypted message is received that requires the same key and when a stored key is not found, the received key can be decrypted. This allows for faster processing of the received message thereby avoiding having to decrypt an

already decrypted key, but still allows the key to be changed and decrypted when necessary to meet security requirements. The cited references do not disclose this novel caching/decrypting feature.

Independent claim 31 recites *receiving an encrypted message; and, decrypting the encrypted message with a stored dialog session key, if a matching service pair security header, a matching key exchange key header and a matching dialog session key header associated with the encrypted message have been stored.* The subject claims discloses a time saving feature that allows the message to be decrypted using a stored dialog session key when the header information of the received message is matched. This allows for bypassing decryption of the various keys avoiding the associated processing overhead. Helland, Bresson, and IETF fail to disclose the various headers disclosed in the subject claim and also fail to disclose a matching mechanism to avoid decryption of all of the keys associated with the headers as taught in the subject claim.

Independent claim 35 recites *a key exchange key header comprising an asymmetrically encrypted key exchange key; a dialog session key header comprising a dialog session key encrypted with the key exchange key; and, a message body field comprising a message encrypted with the dialog session key.* As discussed above, the cited reference fails to disclose a multi-level key encryption scheme and more specifically fails to disclose employing an asymmetrically encrypted key to encrypt a lower level key that is employed to encrypt a message body.

In view of at least the foregoing discussion, applicant's representative respectfully submits that Helland, Bresson, and IETF, alone or in combination fails to teach or suggest all limitations of applicants' invention as recited in independent claims 1, 17, 26, 31 and 35 (and claims 2-16, 18-25, 27-29 and 31-34 that respectfully depend there from), and thus fails to make obvious the subject claimed invention. Accordingly, this rejection should be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP624US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/

Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731